Amendments to the Specification

Please replace paragraph **[0001]** with the following marked-up replacement paragraph:

-- The present invention is related to commonly-assigned U. S. Patent 7,346,923 (serial ~~Patent _____ (serial~~ number 10/719,490, filed November 21, 2003), which is titled "Federated Identity Management within a Distributed Portal Server". This commonly-assigned invention is referred to herein as "the related invention" and is hereby incorporated herein by reference. --

Please replace paragraph **[0038]** with the following marked-up replacement paragraph:

-- Thus, according to the related invention, once the local trust proxy determines that the user is authenticated for the local security domain, this local trust proxy passes information pertaining to the user's authenticated credentials to the trust proxy for each of the remote security domains. Credential mapping operations are then carried out in the remote security domains to determine the user's local credentials for each of the remote security domains. For example, the user might have a user identifier ("user ID") of "Employee1234" in the local domain; a user ID of "Account5678" in the banking domain; and a user ID of "Portfolio543" in the stock portfolio domain, where all of these identifiers belong to the same user. Different underlying security techniques may be used in the different security domains as well. Credential mapping eliminates the need for the user to provide each of these different user IDs (and their corresponding password) to the aggregation point, and allows each security domain to carry out its own security techniques to authenticate the user with [[that]] the user credentials which have been established for that security domain. --

Please replace paragraph **[0039]** with the following marked-up replacement paragraph:

-- Authentication results within each domain are passed to the appropriate service deployed within that domain (e.g., informing the bank account service as to whether the bank account information for the user should be invoked, in the example, where this bank account service operates to provide a view that will be aggregated at the aggregation point-of-contact with the employee benefits information and stock portfolio information). These results are also sent to the aggregation point-of-contact. If the aggregation point-of-contact receives information that the user is not authenticated (or not authorized) for using services in any of the security domains, then the view of the corresponding service will not be included in the aggregated view (and the corresponding service, which also receives this information, should not supply content to the aggregator). In preferred embodiments of the related invention, the aggregation point-of-contact provides the aggregated views as a portal page and the remote services are Web services-based portlets; the local service is preferably deployed as a portlet as well. The related invention therefore enables seamlessly integrating Web services-based portlets, which may rely on different security mechanisms and which may be deployed by various third parties, within a common portal page or other aggregation. --

Please replace paragraph **[0049]** with the following marked-up replacement paragraph:

-- Thus, when distributed portal 210 publishes a message requesting authentication of user 205 in the local security domain 275, local trust proxy 235 communicates with local authentication service 240, which performs the authentication. Assuming the user is authenticated locally, results of the authentication are passed by local trust proxy 235 to remote

trust proxies 220 and 250, which in turn communicate with their own local authentication services (identified in Fig. 2 as remote authentication services 225 and 255, respectively) to determine whether the user is authenticated in the remote domains. (As disclosed in the related invention, the user for which services are to be federated may have varying security identities within the different security domains 270, [[287]] 275, 280. Thus, credential mapping may be carried out in the remote domains when authenticating the user for that domain.) --

Please replace paragraph **[0056]** with the following marked-up replacement paragraph:

-- Fig. 3 shows participants on a generalized routing path used to transmit a SOAP message between a message sender 300 and an ultimate message receiver 340, as well as several intermediaries 310, 320, 330 that may be encountered along the path to message receiver 340. Intermediaries 310, 320, 330 are referred to in Fig. 3 using the notation "TP/SI", an abbreviation for "trust proxy/SOAP intermediary", indicating that these components may serve as trust proxies of the type discussed above and/or as SOAP nodes that route a message along the path from sender 300 to receiver 340. For example, TP/SI 310 might represent the local trust proxy 235 of Fig. 2, while TP/SI 320 represents remote proxy 220 and TP/SI 330 represents remote authentication service 225; and in this example, message sender 300 corresponds to generic portlet proxy 215 (operating on behalf of distributed portal 210) and message receiver 340 corresponds to remote portlet 230. (Note that when nodes 300 - 340 are identified in Fig. 3 as SOAP nodes, this implies that a service description is available for each node. In alternative embodiments, nodes other than SOAP nodes may be supported.)

Please replace paragraph **[0057]** with the following marked-up replacement paragraph:

-- To ensure that messages sent among the security domains are protected, security-sensitive portions of the messages are preferably encrypted before transmission. A particular intermediary may need access to one or more of these security-sensitive portions of a transmitted message for performing functions locally. For example, when an authentication request is transmitted from generic portlet proxy 215 to local trust proxy 235, the local trust proxy needs to determine what is being requested of the local environment and also which, if any, remote trust proxies it must contact to perform remote authentication. If information needed by local trust proxy 235 in the message sent from generic portlet proxy 215 is encrypted, then local trust proxy 235 must be able to decrypt that information. Local trust proxy 235 can then evaluate that decrypted information and, upon determining that remote trust proxies 220 and 250 must be contacted, sends messages to those trust proxies wherein encryption is used to protect security-sensitive information as it travels to the remote security domains. (Similarly, trust proxies in the remote domains may need to forward information to other receivers. Preferably, each trust proxy authenticates a digital signature on received messages to ensure the messages ~~message~~ are authentic prior to carrying out further operations, as in the prior art.) --

Please replace paragraph **[0069]** with the following marked-up replacement paragraph:

-- As shown in Block 420, after determining the message route, a quality of protection overlay is then performed. In preferred embodiments, this comprises harvesting policy information for all intermediaries that will be encountered along the selected route to the ultimate message receiver. Preferably, a WSDL specification for each of the intermediaries is

consulted, and policy information of the intermediary is thereby identified. Or, roles of each intermediary may be used when locating appropriate policy information. For example, policy may specify that an intermediary in the role of routing entity is allowed only to view information pertaining to the selected route for the message or perhaps a subset of the route (such as an identification of the next hop), while intermediaries in the role of trust proxy are allowed to view additional information. As another example, policy may specify that a trusted entity that caches content should be allowed to decrypt selected portions of encrypted content within a transmitted message; or, if authentications are to be cached, as discussed earlier, then an encrypted message portion preferably contains the authentication information to be decrypted by the trusted entity that performs this authentication caching. This policy information as to which message portions should be accessible may be referred to as "entitlements" of message recipients. --

Please replace paragraph **[0082]** with the following marked-up replacement paragraph:

-- The message preferably contains an element that an arbitrary message recipient (including intermediaries) can consult to determine where to find message portions that are to be decrypted by the message recipient. Obviously, this particular element should be specified in the clear. In Fig. 6, a "<securityHeader>" element 610 is provided for this purpose, and contains a set of "<msgReceiver>" elements 615, 620 ... which each specify information about a particular intended receiver or a set of receivers described by a particular role. In the example, a particular message receiver is identified in element 615 by its IP address and port number ~~(i.e., "1.2.3.4:99")~~ (i.e., "1.2.3.4:999"), and a set of receivers is identified in element 620 by their role "remote trust proxy" (for purposes of illustration). A "<receiverID>" and "<receiverRole>" tag,

respectively, are used for these different types of information. Each "<msgReceiver>" element also contains a "<receiverTagName>" element that identifies the name of the tag where this intended receiver's security-protected information may be found. Thus, the receiver identified by IP address and port number in element 615 can find its protected information in the tag named "<1234Tag>", which is shown at reference number 625. Similarly, the receiver(s) identified by role in element 620 can find protected information in the tag named "<RTPTag>" (where "RTP" is used as an abbreviation for "remote trust proxy"), and this tag is shown at reference number 630. In tags 625 and 630, the contained information may be encrypted; it may contain digital signature information; and so forth. (As will be obvious once the teachings disclosed herein are known, information of the type illustrated in Fig. 6 may be presented in a number of different ways without deviating from the scope of the present invention.) --

Please replace paragraph **[0088]** with the following marked-up replacement paragraph:

-- Commonly-assigned and co-pending U. S. Patent Application 20030135628 (serial number 10/047,811; attorney docket ~~RSW920030199US1~~ RSW920010199US1), which is titled "Provisioning Aggregated Services in a Distributed Computing Environment", discloses techniques that enable heterogeneous identity systems to be joined in the dynamic, run-time Web services integration environment. This application, referred to herein as "the provisioning invention", is hereby incorporated herein by reference. A provisioning interface was disclosed in the provisioning invention to enable automatically and dynamically federating the heterogeneous identity systems which may be in use among the services which are aggregated as a composite service. Techniques disclosed therein allow users (whether human or programmatic) to be

seamlessly authenticated and authorized, or "identified", for using the dynamically-integrated services. According to the provisioning invention, this seamless identification may be provided using a single sign-on, or "unified login", for an aggregated service, wherein the provisioning interface of the aggregated service can be used to solicit all required information from a user at the outset of executing the aggregated service. A "stacking" approach was described whereby user passwords (or other credentials, equivalently, such as tickets or digital certificates) to be provided to the sub-services of an aggregated service are encrypted for securely storing. The sub-services are invoked in a specified order during execution, according to a definition that is preferably specified in the Web Services Flow Language ("WSFL"), and the stacked passwords are then unstacked and presented to the appropriate authentication or authorization sub-service.

--